Claims

1. A computer program product for automatically determining if a packet is a new, exploit candidate, said program product comprising:

a computer readable medium;

first program instructions to determine if said packet is a known exploit or portion thereof;

second program instructions to determine if said packet is network broadcast traffic presumed to be harmless; and

third program instructions to determine if said packet is network administration traffic; wherein

if said packet is said known exploit or portion thereof, network broadcast traffic, or network administration traffic, said packet is not considered a new, exploit candidate; and

if said packet is not said known exploit or portion thereof, network broadcast traffic, or network administration traffic, said packet is an exploit candidate; and

said first, second and third program instructions are recorded on said medium.

2. A computer program product as set forth in claim 1 further comprising:

fourth program instructions to determine if said packet is web crawler traffic; and wherein if said packet is said known exploit or portion thereof, network broadcast traffic, network administration traffic or web crawler traffic, said packet is not considered a new, exploit candidate; and

if said packet is not said known exploit or portion thereof, network broadcast traffic, network administration traffic or web crawler traffic, said packet is an exploit candidate; and

said fourth program instructions are recorded on said medium.

3. A computer program product as set forth in claim 1 wherein said first program instructions determine if said packet is a known exploit or portion thereof by searching said packet for a known signature of said known exploit.

4. A computer program product as set forth in claim 1 wherein said first program instructions determine if said packet is a known exploit by comparing an identity of said packet to one or more identities, sent by an intrusion detection system, of respective packet(s) which said intrusion detection system determined to contain a known exploit or portion thereof.

5. A computer program product as set forth in claim 1 wherein said packet was received by a computing device at an unused IP address, and said program product is executed at said computing device.

6. A computer program product as set forth in claim 5 wherein said computing device is a honeypot.

7. A computer program product as set forth in claim 1 further comprising:

fourth program instructions to determine if said packet is broadcast traffic, and wherein if said packet is said known exploit or portion thereof, broadcast traffic, or network administration traffic, said packet is not considered a new, exploit candidate; and

if said packet is not said known exploit or portion thereof, broadcast traffic, or network administration traffic, said packet is an exploit candidate; and

said fourth program instructions are recorded on said medium.

8. A computer program product as set forth in claim 7 wherein said fourth program instructions determines if said packet is broadcast traffic based on a gateway IP address and netmask of said packet.

9. A computer program product as set forth in claim 1 wherein said second program instructions determines if said packet is said network broadcast traffic by comparing a protocol of said packet to a list of protocols assumed to be harmless network broadcast traffic.

10. A computer program product as set forth in claim 1 wherein said third program instructions determines if said packet is network administration traffic by comparing an IP protocol and IP address of said packet to a list of combinations of IP protocols and IP addresses assumed to be network administration traffic.

11. A computer program product as set forth in claim 2 wherein said forth program instructions determines if said packet is web crawler traffic by comparing an IP address of said packet to a list of IP addresses of known web crawlers.

12. A computer program product as set forth in claim 1 wherein if said packet is not said known exploit, network broadcast traffic, or network administration traffic, further comprising fourth program instructions to identify a sequence of packets including the first said packet, said sequence of packets being a new, exploit candidate; and wherein

said forth program instructions are recorded on said medium.

13. A computer system for automatically determining if a packet is a new, exploit candidate, said system comprising:

means for determining if said packet is a known exploit or portion thereof;

means for determining if said packet is network broadcast traffic presumed to be harmless; and

means for determining if said packet is network administration traffic; wherein

if said packet is said known exploit or portion thereof, network broadcast traffic, or network administration traffic, said packet is not considered a new, exploit candidate; and

if said packet is not said known exploit or portion thereof, network broadcast traffic, or network administration traffic, said packet is an exploit candidate.

14. A computer system as set forth in claim 13 further comprising:

means for determining if said packet is web crawler traffic; and wherein

if said packet is said known exploit or portion thereof, network broadcast traffic, network administration traffic or web crawler traffic, said packet is not considered a new, exploit candidate; and if said packet is not said known exploit or portion thereof, network broadcast traffic, network administration traffic or web crawler traffic, said packet is an exploit candidate.

15. A computer system as set forth in claim 13 wherein said packet was received by said computer system at an unused IP address.

16. A computer system as set forth in claim 13 wherein said computer system is a honeypot.

17. A computer program product for automatically determining if a packet is a new, exploit candidate, said program product comprising:

a computer readable medium;

first program instructions to determine if said packet is a known exploit or portion thereof;

second program instructions to determine if said packet is network broadcast traffic presumed to be harmless; and

third program instructions to determine if said packet is another type presumed or known from experience to be harmless; wherein

if said packet is said known exploit or portion thereof, network broadcast traffic, or said other type, said packet is not considered a new, exploit candidate; and

if said packet is not said known exploit or portion thereof, network broadcast traffic, or said other type, said packet is an exploit candidate; and

said first, second and third program instructions are recorded on said medium.

18. A computer program product as set forth in claim 17 wherein said first program instructions determine if said packet is a known exploit or portion thereof by searching said packet for a known signature of said known exploit.

19. A computer program product as set forth in claim 17 wherein said first program instructions determine if said packet is a known exploit by comparing an identity of said packet to one or more identities, sent by an intrusion detection system, of respective packet(s) which said intrusion detection system determined to contain a known exploit or portion thereof.

20. A computer program product as set forth in claim 17 wherein said second program instructions determines if said packet is said network broadcast traffic by comparing a protocol of said packet to a list of protocols assumed to be harmless network broadcast traffic.